

# EMPIRE UNIX System Management Agent

---

10/10/96

Prepared for  
DISA

by  
J G Van Dyke & Associates

# Segment Abstract

Empire UNIX System Management Agent V2.0.0.01

## Purpose:

The UNIX System Management Agent provides powerful UNIX management via the industry standard Simple Network Management Protocol, (SNMP). The agent enables remote Network Management Stations (NMS) to access important information about the system's configuration, status, performance, users, processes, file systems and much more. In addition the agent includes intelligent self-monitoring capabilities for exception-reporting management that eliminates the need for excessive polling.

## Example:

The intelligent capability of the agent monitors disk space. If the disk space on a partition exceeds 95% the agent will send a trap to notify the System/Network Manager.

Specifically the GMC utilizes the agent to monitor the performance of vital GCCS servers and applications. This capability will be extended to the local System Administrator.

# Table of Contents

Version Description Document (VDD) Revision 2.0.0.01 .....	1
Software Requirements Specification (SRS) .....	2
Operators Manual (OM) .....	2
Software Test Plan (STP) .....	2
Software Test Description (STD) .....	3
Known Problem Lists (KPL) .....	3
Installation Procedures (IP) .....	3

# Version Description Document (VDD) Revision 2.0.0.01

## **Empire Technologies, Inc., UNIX Systems Management Agent, Version 2.0.0**

Empire UNIX Systems Management Agent implements MIB-II (RFC 1213), Empire's UNIX Management MIB, and the Host Resources (RFC 1514) MIB. The UNIX MIB defines groups for kernel and systems parameters, boot configuration, network, streams, and I/O buffer statistics, kernel performance statistics, and an object monitoring table. The Host MIB includes information on storage areas such as file systems and disk partitions, running and installed software, and the host system's devices such as keyboard, disks, and network cards. The agent enables remote network management stations (NMS) to access important information such as the above mentioned metrics. The agent includes self-monitoring capability for exception reporting management that eliminates the need for excessive polling. The UNIX Systems Agent interoperates with SNMP NMS platforms such as SunNet Manager and others. A daemon, started at boot up, handles the trap forwarding to the management station.

This revision supersedes all previous revisions of the UNIX Systems MGMT Agent segment. Deinstall all previous revisions of this segment before installing this revision (version 2.0.0.01).

### **System Requirements**

The UNIX Systems Management Agent will operate on Sun SPARC platforms or clones:

- running either Sun OS or Solaris 2.x.
- 8 megabytes of RAM is the minimum amount of memory required.
- 1000 kilobytes of disk space is required

### **HR MIB**

The Host Resources MIB defines a uniform set of objects useful for the management of host computers. Host computers are independent of the operating system, network services, or software application. Objects are common across many computer system architectures.

### **Empire MIB**

The Empire MIB defines a detailed set of metrics covering host system information, mounted devices, kernel configuration, boot configuration,

streams group, user information, group information, process information, who information, remote command execution, performance monitoring, kernel performance statistics, interprocess communication, message buffer allocation, stream buffers, I/O buffer cache, monitor table, RPC group, and NFS group.

### **Traps**

The file `snmpd.empire.conf` defines both access communities and trap communities which tell the agent where to send the trap messages. The agent can be configured to send traps to any number of managers.

## **Software Requirements Specification (SRS)**

See EMPIRE Technologies System Management User's Guide.

## **Operators Manual (OM)**

The UNIX System Management Agent is a system daemon that runs on a UNIX host. Operation of the agent consists of starting the daemon on the host system. This is accomplished on the host system during boot-up by the `"/etc/rc2.d/S99empuma"` script or from the command line using the `"/h/COTS/EMPIRE/config/S99empuma start"` command.

The `snmpd` daemon requires a license key to run and will not start until one is provided. During the segment installation a license key request is generated and mailed back to the OSF Hotline. The Hotline personnel will acquire the license from the vendor and update the `"/h/COTS/EMPIRE/config/snmpd.empire.license"` file using the `netadmin` account. The system administrator specified during the install will then be notified that the agent is ready to run.

## **Software Test Plan (STP)**

Test and acceptance of the Agent consists of the following steps.

1. Successful installation of the UNIX System Management Agent segment.
2. Successful installation of the UNIX System Management Agent license file.

3. Successful starting of the Agent.

## Software Test Description (STD)

Not Applicable

## Known Problem Lists (KPL)

None

## Installation Procedures (IP)

UNIX System Management Agent

The following script is an example of the installation process for the UNIX System Management agent. Suggested responses are enclosed in braces "{}":

1. Ensure that you are user 'sysadmin' {%su - sysadmin}
2. Run SAInstaller {%SAInstaller -debug}
3. From the SEGMENTS CURRENTLY INSTALLED list select the previous version of the 'UNIX Systems MGMT Agent' segment
4. Click on 'DE-INSTALL'
5. Load segment tape into drive
6. Click on 'SELECT MEDIA'
7. Select host and devices  
{REMOTE NAME   zorro  
  DEVICE OTHER   /dev/rmt/0mbn}
8. Select 'READ TABLE OF CONTENTS'
9. From the Table of Contents list select 'UNIX Systems MGMT Agent'
10.    Select 'INSTALL'

11. When the `PostInstall.EMPIRE XTERM` window pops up, answer the following questions:

If it is necessary to create an account for user “netadmin” you will be prompted for a password. A recommended password is ‘netadmin1’. If you choose a different password, please notify the OSF Hotline of the new password by sending email to “netadmin@madrid.osf.disa.smil.mil”.

**Who is the system administrator for this machine?**

{ Enter the name of the designated system administrator. This person will be contacted by the OSF Hotline once the license is installed. }

**Enter the DSN phone # for this system administrator:**

{ Enter the DSN phone # for the person listed above }

**Where is this system located (site, bldg, room, etc)?**

{ Enter the information corresponding to the facility }

**Are these entries correct? <y/n>**

{ Enter y or n, then <RETURN>. If you enter n then you will have an opportunity to re-enter the information }

12. At the end of the installation process, an email will be sent to the OSF and GMC with the license key checksum. The CM personnel will contact the vendor, acquire the necessary license and then notify the system administrator.
13. Once the segment is licensed, verify the agent started successfully using the “% ps -aef | grep snmpd” command and check that the snmpd process is running.
15. If no errors were encountered exit the SAInstaller; otherwise, notify the GMC of any problems.